Interference Search [redacted] 09/871,084

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	0	processor.clm. and "operating mode".clm. and access.clm. and lock.clm. and override.clm. and register.clm. and secure.clm.	US-PGPUB; USPAT	OR	OFF	2005/11/22 15:32
L2	0	processor.clm. and mode.clm. and access.clm. and lock.clm. and override.clm. and register.clm. and secure.clm.	US-PGPUB; USPAT	OR	OFF	2005/11/22 15:32
L3	0	processor.clm. and mode.clm. and access.clm. and lock.clm. and register.clm. and secure.clm.	US-PGPUB; USPAT	OR	OFF	2005/11/22 15:32
L4	2	mode.clm. and access.clm. and lock.clm. and register.clm. and secure.clm.	US-PGPUB; USPAT	OR	OFF	2005/11/22 15:33
L5	0	mode.clm. and access.clm. and lock.clm. and register.clm. and secure.clm. and processor.clm.	US-PGPUB; USPAT	OR	OFF	2005/11/22 15:33
L6	0	mode.clm. and access.clm. and lock.clm. and register.clm. and secure.clm. and hardware.clm.	US-PGPUB; USPAT	OR	OFF	2005/11/22 15:34
L7	0	mode.clm. and access.clm. and lock.clm. and register.clm. and secure.clm. and bit.clm.	US-PGPUB; USPAT	OR	OFF	2005/11/22 15:34
L8	7	mode.clm. and access.clm. and register.clm. and secure.clm. and bit.clm.	US-PGPUB; USPAT	OR	OFF	2005/11/22 15:34

Search [redacted] 09/871,084

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	0	processor.clm. and "operating mode".clm. and access.clm. and lock.clm. and override.clm. and register.clm. and secure.clm.	US-PGPUB; USPAT	OR	OFF	2005/11/22 15:32
L2	0	processor.clm. and mode.clm. and access.clm. and lock.clm. and override.clm. and register.clm. and secure.clm.	US-PGPUB; USPAT	OR	OFF	2005/11/22 15:32
L3	0	processor.clm. and mode.clm. and access.clm. and lock.clm. and register.clm. and secure.clm.	US-PGPUB; USPAT	OR	OFF	2005/11/22 15:32
L4	2	mode.clm. and access.clm. and lock.clm. and register.clm. and secure.clm.	US-PGPUB; USPAT	OR	OFF	2005/11/22 15:33
L5	0	mode.clm. and access.clm. and lock.clm. and register.clm. and secure.clm. and processor.clm.	US-PGPUB; USPAT	OR	OFF	2005/11/22 15:33
L6	0	mode.clm. and access.clm. and lock.clm. and register.clm. and secure.clm. and hardware.clm.	US-PGPUB; USPAT	OR	OFF	2005/11/22 15:34
L7	0	mode.clm. and access.clm. and lock.clm. and register.clm. and secure.clm. and bit.clm.	US-PGPUB; USPAT	OR	OFF	2005/11/22 15:34
L8	7	mode.clm. and access.clm. and register.clm. and secure.clm. and bit.clm.	US-PGPUB; USPAT	OR	OFF	2005/11/22 15:37
L9	405	713/194	US-PGPUB; USPAT	OR	OFF	2005/11/22 15:35
L10	449	713/172	US-PGPUB; USPAT	OR	OFF	2005/11/22 15:35
L11	1472	713/172 or 713/182 or 726/34 or 257/922	US-PGPUB; USPAT	OR	OFF	2005/11/22 15:36
L12	1805	11 or 9	US-PGPUB; USPAT	OR	OFF	2005/11/22 15:36
L13	1905	mode and access and register and secure and bit and hardware and lock	US-PGPUB; USPAT	OR	OFF	2005/11/22 15:37
L14	1905	13 and register$2	US-PGPUB; USPAT	OR	OFF	2005/11/22 15:37
L15	21	14 and 12	US-PGPUB; USPAT	OR	OFF	2005/11/22 15:38

Terms used
mode$2 and **access** and **register$2** and **secure** and **bit$1** and **hardware** and **lock**

Found **10,374** of **166,953**

Sort results by: relevance

Display results: expanded form

Save results to a Binder

Search Tips

Open results in a new window

Try an Advanced Search

Try this search in The ACM Guide

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next

Best 200 shown

Relevance scale

1 A study of initialization in Linux and OpenBSD

Catherine Dodge, Cynthia Irvine, Thuy Nguyen

April 2005 **ACM SIGOPS Operating Systems Review**, Volume 39 Issue 2

Publisher: ACM Press

Full text available: pdf(2.02 MB) Additional Information: full citation, abstract, references, index terms

The code that initializes a system can be notoriously difficult to understand. In secure systems, initialization is critical for establishing a starting state that is secure. This paper explores two architectures used for bringing an operating system to its initial state, once the operating system gains control from the boot loader. Specifically, the ways in which the OpenBSD and Linux operating systems handle initialization are dissected.

2 Operating System Structures to Support Security and Reliable Software

Theodore A. Linden

December 1976 **ACM Computing Surveys (CSUR)**, Volume 8 Issue 4

Publisher: ACM Press

Full text available: pdf(3.49 MB) Additional Information: full citation, references, citings, index terms

3 Privacy: Privacy and security in library RFID: issues, practices, and architectures

David Molnar, David Wagner

October 2004 **Proceedings of the 11th ACM conference on Computer and communications security**

Publisher: ACM Press

Full text available: pdf(241.45 KB) Additional Information: full citation, abstract, references, index terms

We expose privacy issues related to Radio Frequency Identification (RFID) in libraries, describe current deployments, and suggest novel architectures for library RFID. Libraries are a fast growing application of RFID; the technology promises to relieve repetitive strain injury, speed patron self-checkout, and make possible comprehensive inventory. Unlike supply-chain RFID, library RFID requires item-level tagging, thereby raising immediate patron privacy issues. Current conventional wisdom su ...

Keywords: RFID, privacy, private authentication, security

4 ARPS: a new real-time computer
Kenneth J. Thurber
October 1976 **ACM SIGARCH Computer Architecture News**, Volume 5 Issue 4
Publisher: ACM Press
Full text available: pdf(1.14 MB) Additional Information: full citation, references, citings

5 RISCY patents
David A. Patterson
September 1988 **ACM SIGARCH Computer Architecture News**, Volume 16 Issue 4
Publisher: ACM Press
Full text available: pdf(1.83 MB) Additional Information: full citation, index terms

6 Fault Tolerant Operating Systems
Peter J. Denning
December 1976 **ACM Computing Surveys (CSUR)**, Volume 8 Issue 4
Publisher: ACM Press
Full text available: pdf(2.69 MB) Additional Information: full citation, references, citings, index terms

7 Formal Models for Computer Security
Carl E. Landwehr
September 1981 **ACM Computing Surveys (CSUR)**, Volume 13 Issue 3
Publisher: ACM Press
Full text available: pdf(2.98 MB) Additional Information: full citation, references, citings, index terms

8 Shake 'em, but don't crack 'em: Shake them up!: a movement-based pairing protocol for CPU-constrained devices
Claude Castelluccia, Pars Mutaf
June 2005 **Proceedings of the 3rd international conference on Mobile systems, applications, and services MobiSys '05**
Publisher: ACM Press
Full text available: pdf(295.02 KB) Additional Information: full citation, abstract, references

This paper presents a new pairing protocol that allows two CPU-constrained wireless devices Alice and Bob to establish a shared secret at a very low cost. To our knowledge, this is the first software pairing scheme that does not rely on expensive public-key cryptography, out-of-band channels (such as a keyboard or a display) or specific hardware, making it inexpensive and suitable for CPU-constrained devices such as sensors.

In the described protocol, Alice can send the secre ...

9 Considerations for new tactical computer systems
Jon C. Strauss, Kenneth J. Thurber
March 1977 **ACM SIGARCH Computer Architecture News , Proceedings of the 4th annual symposium on Computer architecture ISCA '77**, Volume 5 Issue 7
Publisher: ACM Press
Full text available: pdf(513.31 KB) Additional Information: full citation, abstract, references, index terms

The real-time command and control environments characteristic of tactical military systems and industrial process control systems place unique and conflicting design requirements on a support computer system. These requirements include fast context switching, selective protection of programs and their files, controlled sharing of program and files, high processing speed, flexible, yet fast priority structure for interrupts and program execution, flexible high-speed I/O and flexible intercom ...

10 Some formal language aspects of MARY

Mark Rain

July 1972 **ALGOL Bulletin**, Issue 34

Publisher: Computer History Museum

Full text available: pdf(1.51 MB) Additional Information: full citation, index terms

11 A Tutorial on Algol 68

Andrew S. Tanenbaum

June 1976 **ACM Computing Surveys (CSUR)**, Volume 8 Issue 2

Publisher: ACM Press

Full text available: pdf(2.92 MB) Additional Information: full citation, references, citings, index terms

12 Cost profile of a highly assured, secure operating system

Richard E. Smith

February 2001 **ACM Transactions on Information and System Security (TISSEC)**, Volume 4 Issue 1

Publisher: ACM Press

Full text available: pdf(165.98 KB) Additional Information: full citation, abstract, references, citings, index terms

The Logical Coprocessing Kernel (LOCK) began as a research project to stretch the state of the art in secure computing by trying to meet or even exceed the "A1" requirements of the Trusted Computer System Evaluation Criteria (TCSEC). Over the span os seven years, the project was transformed into an effort to develop and deploy a product: the Standard Mail Guard (SMG). Since the project took place under a US government contract, the development team needed to maintain detailed re ...

Keywords: LOCK (Logical Coprocessing Kernel), security kernels

13 HIDE: an infrastructure for efficiently protecting information leakage on the address bus

Xiaotong Zhuang, Tao Zhang, Santosh Pande

October 2004 **ACM SIGPLAN Notices , ACM SIGOPS Operating Systems Review , ACM SIGARCH Computer Architecture News , Proceedings of the 11th international conference on Architectural support for programming languages and operating systems ASPLOS-XI**, Volume 39 , 38 , 32 Issue 11 , 5 , 5

Publisher: ACM Press

Full text available: pdf(216.31 KB) Additional Information: full citation, abstract, references, citings, index terms

XOM-based secure processor has recently been introduced as a mechanism to provide copy and tamper resistant execution. XOM provides support for encryption/decryption and integrity checking. However, neither XOM nor any other current approach adequately addresses the problem of information leakage via the address bus. This paper shows that without address bus protection, the XOM model is severely crippled. Two realistic attacks

are shown and experiments show that 70% of the code might be cracked ...

Keywords: address bus leakage protection, secure processor

14 SOS: a monitor-based operating system for instruction

D. E. Boddy

December 1988 **ACM SIGPLAN Notices**, Volume 23 Issue 12

Publisher: ACM Press

Full text available: pdf(769.63 KB) Additional Information: full citation, citings, index terms

15 Specification and analysis of the SNR high-speed transport protocol

Gilbert M. Lundy, H. Alphan Tipici

October 1994 **IEEE/ACM Transactions on Networking (TON)**, Volume 2 Issue 5

Publisher: IEEE Press

Full text available: pdf(1.68 MB) Additional Information: full citation, references, citings, index terms, review

16 Authentication and authorization: Securing passwords against dictionary attacks

Benny Pinkas, Tomas Sander

November 2002 **Proceedings of the 9th ACM conference on Computer and communications security**

Publisher: ACM Press

Full text available: pdf(216.72 KB) Additional Information: full citation, abstract, references, citings, index terms

The use of passwords is a major point of vulnerability in computer security, as passwords are often easy to guess by automated programs running dictionary attacks. Passwords remain the most widely used authentication method despite their well-known security weaknesses. User authentication is clearly a practical problem. From the perspective of a service provider this problem needs to be solved within real-world constraints such as the available hardware and software infrastructures. From a user' ...

17 Virtual machine monitors: Implementing an untrusted operating system on trusted hardware

David Lie, Chandramohan A. Thekkath, Mark Horowitz

October 2003 **Proceedings of the nineteenth ACM symposium on Operating systems principles**

Publisher: ACM Press

Full text available: pdf(280.87 KB) Additional Information: full citation, abstract, references, citings, index terms

Recently, there has been considerable interest in providing "trusted computing platforms" using hardware~---~TCPA and Palladium being the most publicly visible examples. In this paper we discuss our experience with building such a platform using a traditional time-sharing operating system executing on XOM~---~a processor architecture that provides copy protection and tamper-resistance functions. In XOM, only the processor is trusted; main memory and the operating system are not trusted.Our opera ...

Keywords: XOM, XOMOS, untrusted operating systems

18

A nested transaction model for multilevel secure database management systems
Elisa Bertino, Barbara Catania, Elena Ferrari
November 2001 **ACM Transactions on Information and System Security (TISSEC)**, Volume 4 Issue 4
Publisher: ACM Press
Full text available: pdf(560.96 KB) Additional Information: full citation, abstract, references, index terms

This article presents an approach to concurrency control for transactions in a Multilevel Secure Database Management System (MLS/DBMS). The major problem is that concurrency control mechanisms used in traditional DBMSs are not adequate in a MLS/DBMS, since they may be exploited to establish covert channels. The approach presented in this article, which uses single-version data items, is based on the use of nested transactions, application-level recovery, and notification-based locking protocols. ...

Keywords: Nested transactions, concurrency control, covert channels, multilevel secure database management systems

19 Workshop on architectural support for security and anti-virus (WASSA): ChipLock: support for secure microarchitectures
Taeho Kgil, Laura Falk, Trevor Mudge
March 2005 **ACM SIGARCH Computer Architecture News**, Volume 33 Issue 1
Publisher: ACM Press
Full text available: pdf(256.52 KB) Additional Information: full citation, abstract, references, index terms

The increasing need for security has caused system designers to consider placing some security support directly at the hardware level. In fact, this is starting to emerge as an important consideration in processor design, because the performance overhead of supporting security in hardware is usually significantly lower than a complete software solution. In this paper, we investigate integrating some security support into hardware. We show that security support can be added at some acceptable cos ...

20 A formal protection model of security in centralized, parallel, and distributed systems
Glenn S. Benson, Ian F. Akyildiz, William F. Appelbe
August 1990 **ACM Transactions on Computer Systems (TOCS)**, Volume 8 Issue 3
Publisher: ACM Press
Full text available: pdf(2.17 MB) Additional Information: full citation, abstract, references, citings, index terms, review

One way to show that a system is not secure is to demonstrate that a malicious or mistake-prone user or program can break security by causing the system to reach a nonsecure state. A fundamental aspect of a security model is a proof that validates that every state reachable from a secure initial state is secure. A sequential security model assumes that every command that acts as a state transition executes sequentially, while a concurrent security model assumes that multiple commands execut ...

Keywords: access control, concurrency control, distributed system security, operating system security, protection model